Autonomous Threat Hunting With Niddel And Splunk Enterprise Security: Mars Inc. Customer Case Study

Alex Pinto

Chief Data Scientist, Niddel

Greg Poniatowski

Security Service Area Leader, Mars Inc.

.conf2016

splunk>

Who Are We?

- Alex Pinto
  - 15 years as a security consultant
  - 7 Of those years setting up and managing MSSPs and on-prem SOCs
  - 4 years researching Security Data Science focused on network-based detection
  - Patents on machine learning techniques for intrusion detection
- Greg Poniatowski
  - Various security roles in different industries
  - Experience which informed a strong desire to ensure engineering choices are data driven, designed to solve problems, and most importantly – can be effectively operationalized
  - 2+ years at Mars, Inc.

Agenda

1. Introduction To Threat Hunting / Niddel
2. Mars Inc. Splunk Deployment
3. Threat Hunting Examples On Splunk
4. Integrating Niddel Threat Hunting System And ES
5. Conclusion / Takeaways

1. Introduction To Threat Hunting

The State Of Threat Intelligence

Data Feed Providers

The data itself, delivered as a feed or as access to a repository (Manual Integration)

- ✓ Various categories – Context, Black List
- ✓ Free and paid versions
- ✧ Variable QA and false positive ratio
- ✧ Little or no integration support
- ✧ **Not Efficient / Not Effective**

Threat Intelligence Platforms (Including ES Threat Lists)

Focus on collecting and sharing TI

- ✓ Accepts multiple feed categories and sources
- ✓ Focus on integration and API access
- ✧ Limited or no analytics capabilities
- ✧ Limited or no added value besides integration cost
- ✧ **Efficient / Not Effective**

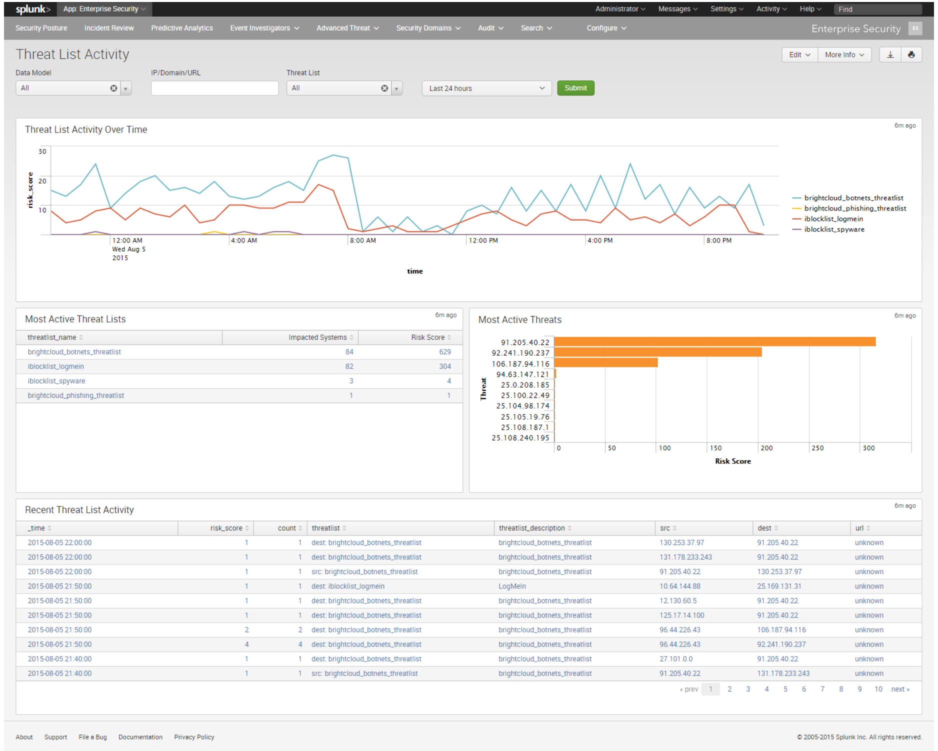
Threat Hunting Platforms

Focus on human-centric analysis TI from multiple sources

- ✓ Manage threat indicators
- ✓ API access
- ✓ Enables complex analysis and dashboards
- ✧ Relies on users with high expertise to conduct any analysis
- ✧ **Not Efficient / Effective**

Existing solutions do not address the problem of analyst overload and hiring gaps: Too many alerts, too many false positives.

Threat Intel On Enterprise Security



Threat List Activity

Most Active Threat Lists

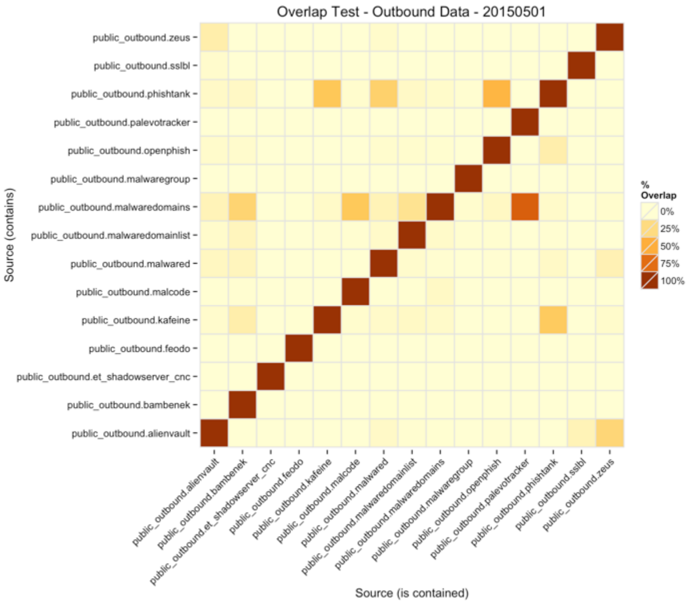
threatlist_name	Impacted Systems	Risk Score
brightcloud_botnets_threatlist	84	629
iblocklist_logmein	82	304
iblocklist_spyware	3	4
brightcloud_phishing_threatlist	1	1

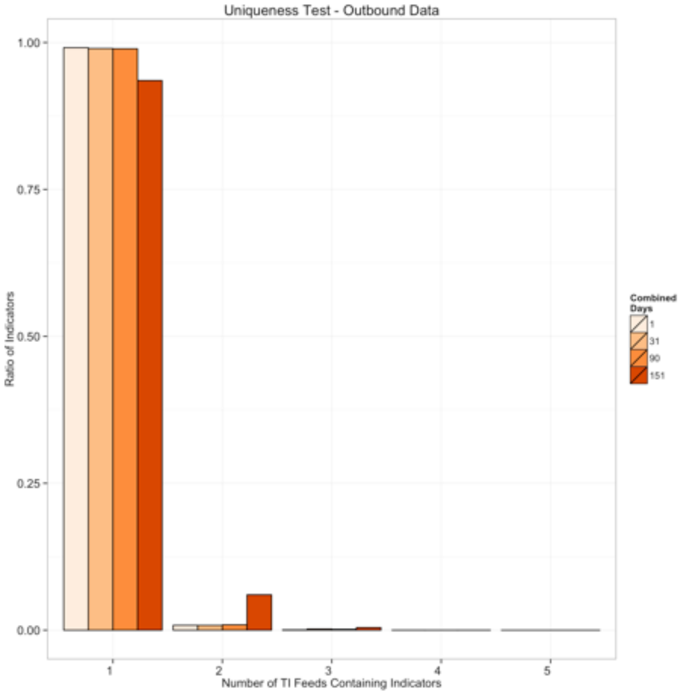
Recent Threat List Activity

_time	risk_score	count	threatlist	threatlist_description	src	dest	url
2015-08-05 22:00:00	1	1	dest: brightcloud_botnets_threatlist	brightcloud_botnets_threatlist	130.253.37.97	91.205.40.22	unknown
2015-08-05 22:00:00	1	1	dest: brightcloud_botnets_threatlist	brightcloud_botnets_threatlist	131.178.233.243	91.205.40.22	unknown
2015-08-05 22:00:00	1	1	src: brightcloud_botnets_threatlist	brightcloud_botnets_threatlist	91.205.40.22	130.253.37.97	unknown
2015-08-05 21:50:00	1	1	dest: iblocklist_logmein	LogMeIn	10.64.144.88	25.169.131.31	unknown
2015-08-05 21:50:00	1	1	dest: brightcloud_botnets_threatlist	brightcloud_botnets_threatlist	12.130.60.5	91.205.40.22	unknown
2015-08-05 21:50:00	1	1	dest: brightcloud_botnets_threatlist	brightcloud_botnets_threatlist	125.17.14.100	91.205.40.22	unknown
2015-08-05 21:50:00	2	2	dest: brightcloud_botnets_threatlist	brightcloud_botnets_threatlist	96.44.226.43	106.187.94.116	unknown
2015-08-05 21:50:00	4	4	dest: brightcloud_botnets_threatlist	brightcloud_botnets_threatlist	96.44.226.43	92.241.190.237	unknown
2015-08-05 21:40:00	1	1	dest: brightcloud_botnets_threatlist	brightcloud_botnets_threatlist	27.101.0.0	91.205.40.22	unknown
2015-08-05 21:40:00	1	1	src: brightcloud_botnets_threatlist	brightcloud_botnets_threatlist	91.205.40.22	131.178.233.243	unknown

- Equivalent to a Threat Intelligence Platform:
  - Pulls the data in (contingent to Add-ons provided by the vendors)
  - Normalizes it
  - Matches it against specific log data searches you may have
- Suffers from all the problems of TIPs in that respect:
  - Very efficient matching on data of dubious quality ☺

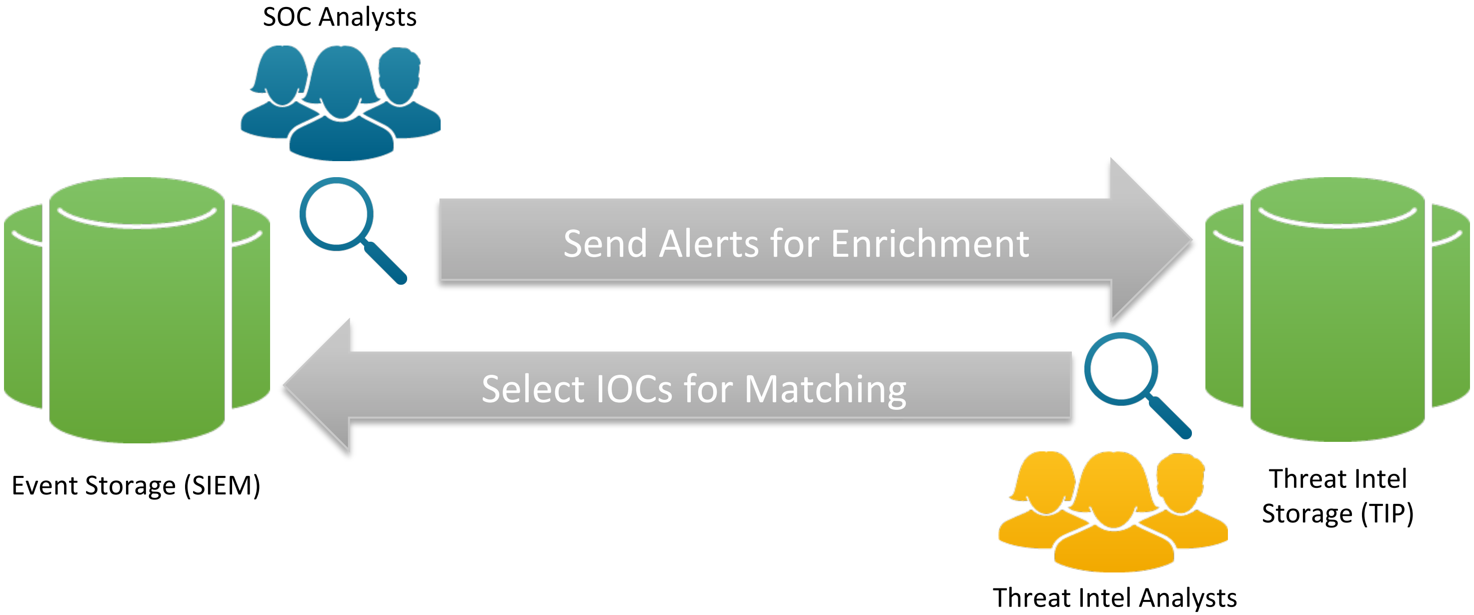
TI – Coverage And Quality Issues





- TIQ-Test (http://www.mlsecproject.org)

The State Of Threat Hunting

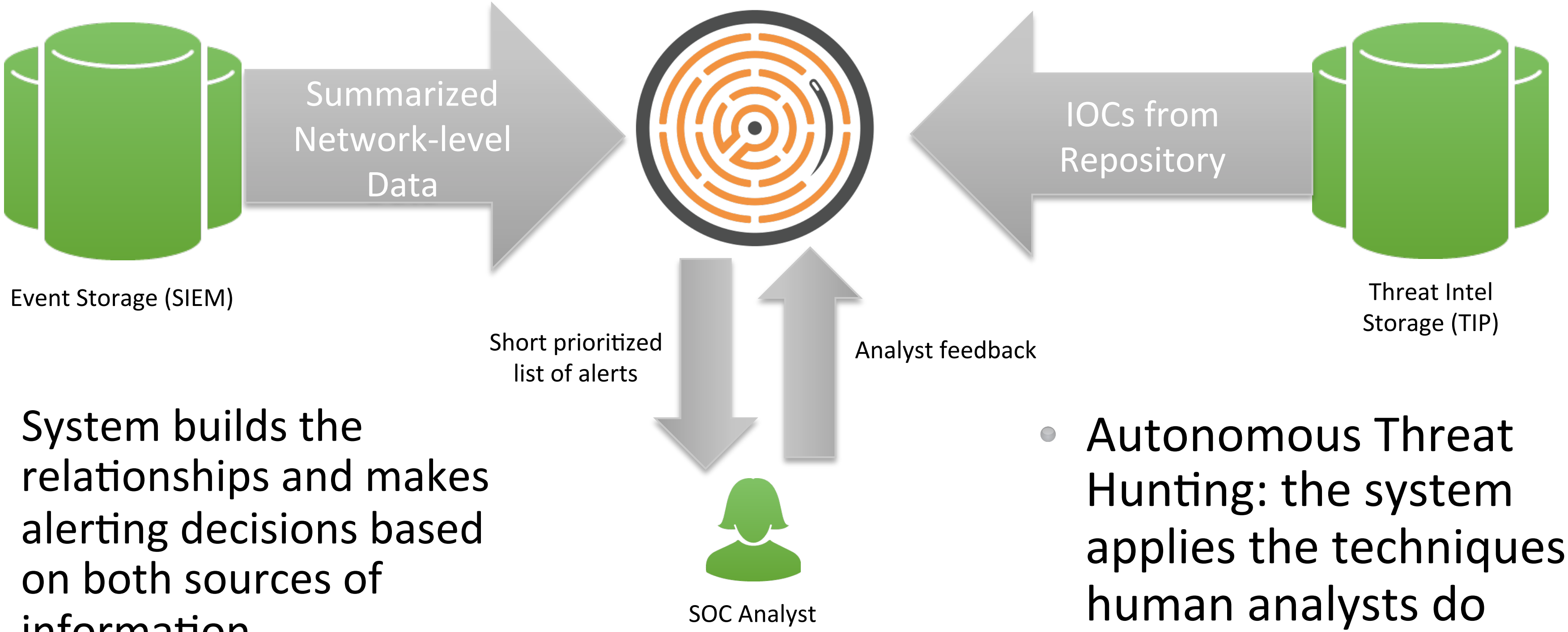


Both have incomplete and biased views

Heavy analyst-centric activity – Needs actual ”teams”

Do not unlock the power of what can be found when the two datasets work together

Putting It All Together - The Niddel Approach



Summarized Network-level Data
IOCs from Repository
Event Storage (SIEM)
Threat Intel Storage (TIP)
Short prioritized list of alerts
Analyst feedback
SOC Analyst

- System builds the relationships and makes alerting decisions based on both sources of information

- Autonomous Threat Hunting: the system applies the techniques human analysts do

2. Mars Inc. Splunk Deployment

Why Splunk Cloud

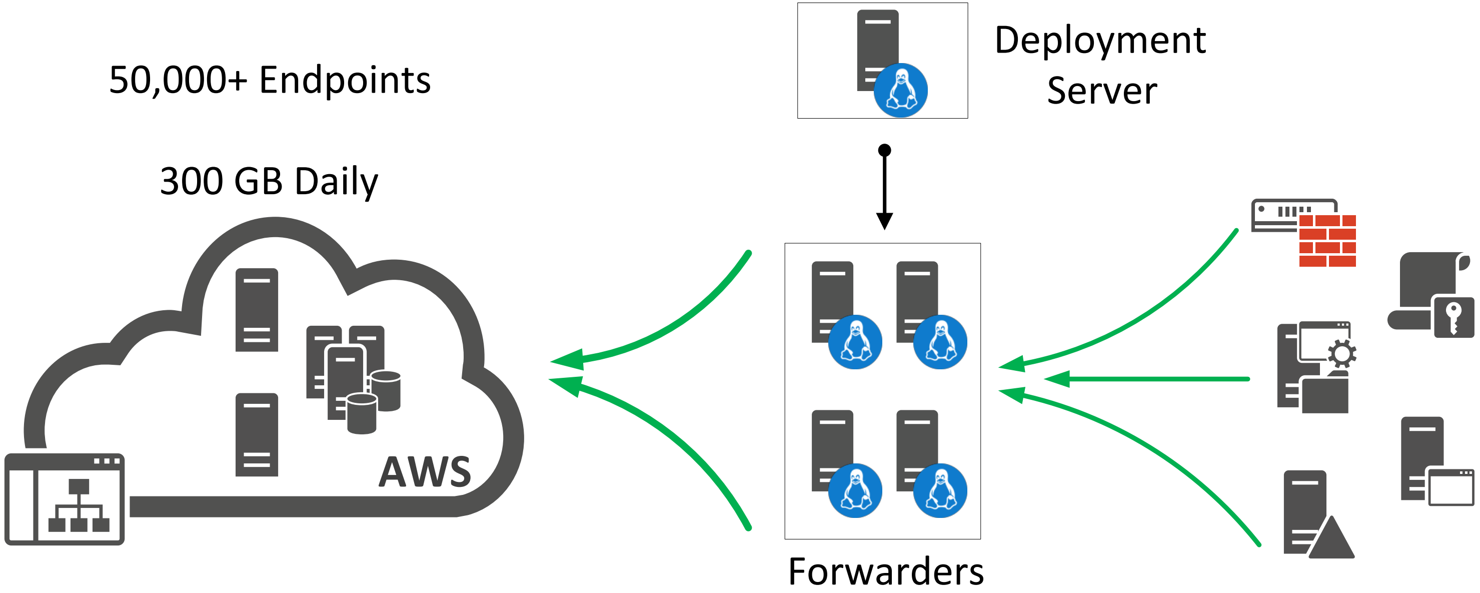
- Small team
- No internal competency building and maintaining a Splunk Enterprise deployment
  - More efficient use of limited resources for developing and operationalizing, not maintenance of infrastructure
- Need for log collection and correlation was acute
  - Lead time to deliver would be drastically reduced through cloud offering
- Better long term strategic fit
  - Get in front of rather than lag behind push to cloud first

Mars Splunk Cloud Deployment

70+ Locations

50,000+ Endpoints

300 GB Daily



Deployment Server

Forwarders

Firewalls

Active Directory

Anti-Virus

Data Protection

File and Print

All production *nix systems

Why Enterprise Security

- Following the selection of Splunk it was natural choice for SIEM tool
- Track incidents internally in Splunk
- Generate operational metrics
- Obviate need to try and develop SIEM capabilities internally

Mars Splunk Enterprise Security

- Triage of endpoint / AV events fairly straightforward
  - Building off early successes by driving greater log collection to refine existing events and build new ones
- Firewall / IPS events proved to be high in volume and difficult for SOC to triage effectively.
  - High occurrence of false positives
  - High absolute numbers of events
  - Clearly the answer was to eliminate those false positives

Splunk ES Identity Management

- Integration with our CMDB and Identity Management solution ensures that Splunk events contain asset and personnel data at search time

- This was an early win made possible through Enterprise Security's Asset and Identity Management capability

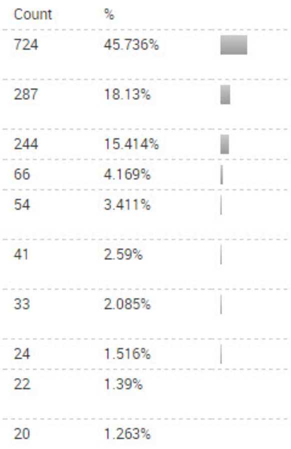
Splunk ES Noise Reduction

- Among our most successful identity and firewall events are those designed to ensure compliance with existing controls and identify configuration issues

- Users being added to highly privileged groups
- Absolute high number of outbound connections
- Unblocked IDS alerts (Inbound and Outbound)
- Absolute high number of blocked connections

Splunk ES Incident Auditing

- Track the value of use cases through classification of resolution
- Measure the efficiency of processes for handling incidents



Count	%
724	45.736%
287	18.13%
244	15.414%
66	4.169%
54	3.411%
41	2.59%
33	2.085%
24	1.516%
22	1.39%
20	1.263%

By reporting on, for example which notable events are resulting in false positives, we can tune them or determine the need for either additional refinement using other data, or new tooling.

Threat Intelligence

- On paper sounds like a solution for the Firewall event volume issue
- No purchase of direct feeds.
- Implementation would not be trivial
- Larger questions arose around how to assess the relative value of different feeds

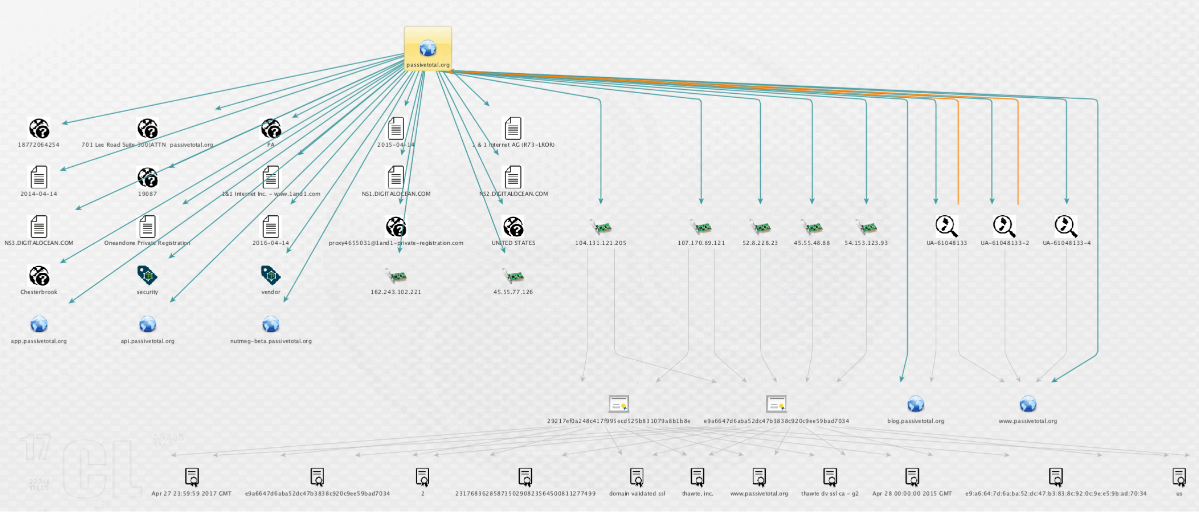
- TI challenges made Niddel a very interesting fit

3. Threat Hunting Examples

.conf2016

splunk>

”Knowledge-based” Threat Hunting

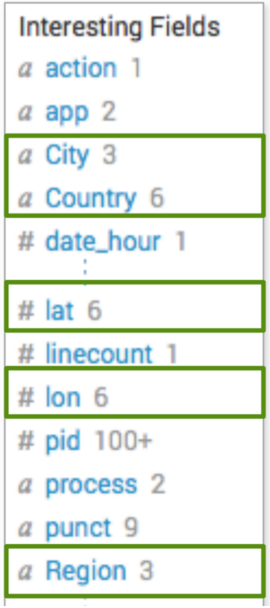


- Holistic view of relationships
  - Allows visibility into “Unknown unknowns”
- All those relationships delineate increased likelihood of maliciousness
- However, negative views (VT, AV) are incomplete for decision making

Threat Hunting – IP Enrichment Data

- IP Addresses:
  - ASN
  - BGP Prefix
  - Datacenter
  - Geolocation
- Splunk has a built-in Geolocation engine with `iplocation` command
- Also, don't forget `geostats` and `geom` for all your pew-pew map needs!

```
| iplocation src_ip
```



Interesting Fields

a action 1

a app 2

a City 3

a Country 6

# date_hour 1

# lat 6

# linecount 1

# lon 6

# pid 100+

a process 2

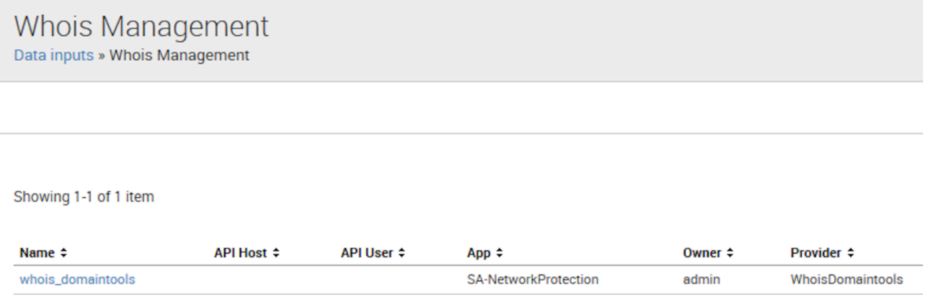
a punct 9

a Region 3

```
| geom geo_countries
```

Threat Hunting – Domain Enrichment Data

- Domain names:
  - Passive DNS
    - Domain siblings
    - Relationships with IP addresses
  - TLS Certificate data
  - WHOIS Information
- Splunk ES has native functionality to integrate with WHOIS providers
- For Passive DNS, only 3rd party for now. I suggest having a look at **Farsight Security** (https://splunkbase.splunk.com/app/3050/)

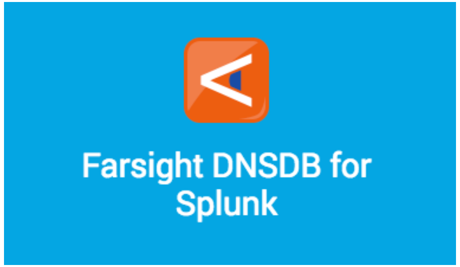


Whois Management

Data inputs » Whois Management

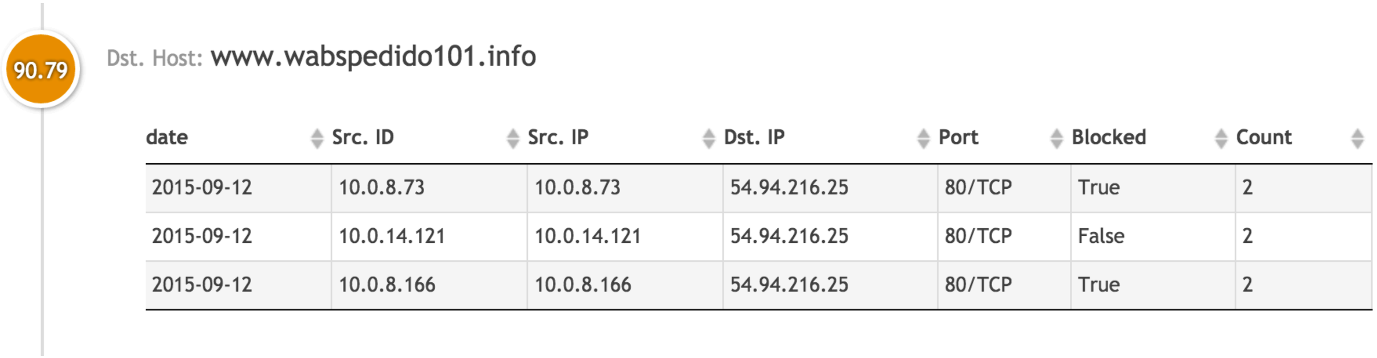
Showing 1-1 of 1 item

Name	API Host	API User	App	Owner	Provider
whois_domaintools			SA-NetworkProtection	admin	WhoisDomaintools



Niddel Magnet – Autonomous Threat Hunting

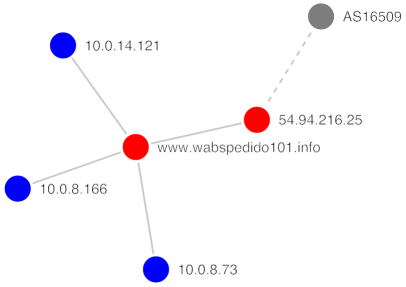
Ex 1: Detecting By Pivoting On pDNS And WHOIS



90.79

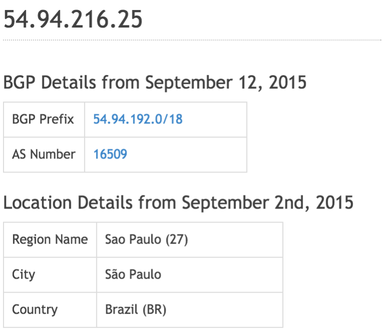
Dst. Host: www.wabspedido101.info

date	Src. ID	Src. IP	Dst. IP	Port	Blocked	Count
2015-09-12	10.0.8.73	10.0.8.73	54.94.216.25	80/TCP	True	2
2015-09-12	10.0.14.121	10.0.14.121	54.94.216.25	80/TCP	False	2
2015-09-12	10.0.8.166	10.0.8.166	54.94.216.25	80/TCP	True	2



- 3 suspicious entries on difference sources shows up with Confidence Level of 90.79 (in a scale of -100 to 100) for investigation
- We can see that 2 of them were blocked, and one other was not
- There are no direct or indirect matches this time. We need to investigate further on the details of the communications, IP address and domain name.

Ex 1: Detecting By Pivoting On pDNS And WHOIS



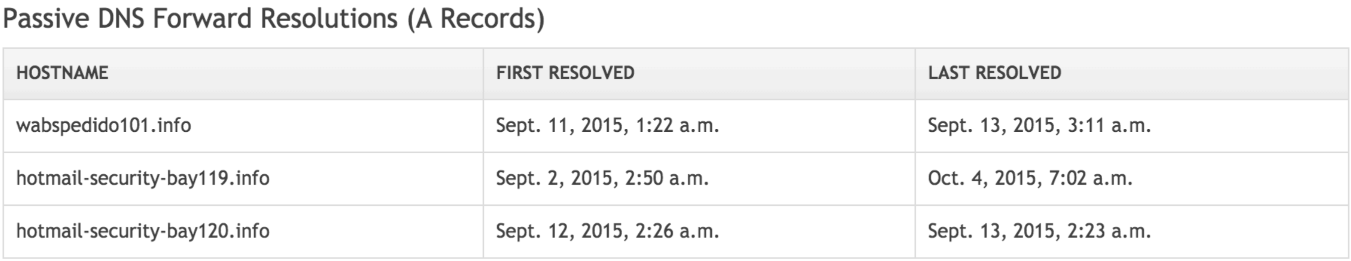
54.94.216.25

BGP Details from September 12, 2015

BGP Prefix	54.94.192.0/18
AS Number	16509

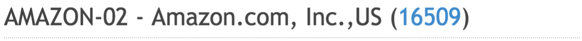
Location Details from September 2nd, 2015

Region Name	Sao Paulo (27)
City	São Paulo
Country	Brazil (BR)



Passive DNS Forward Resolutions (A Records)

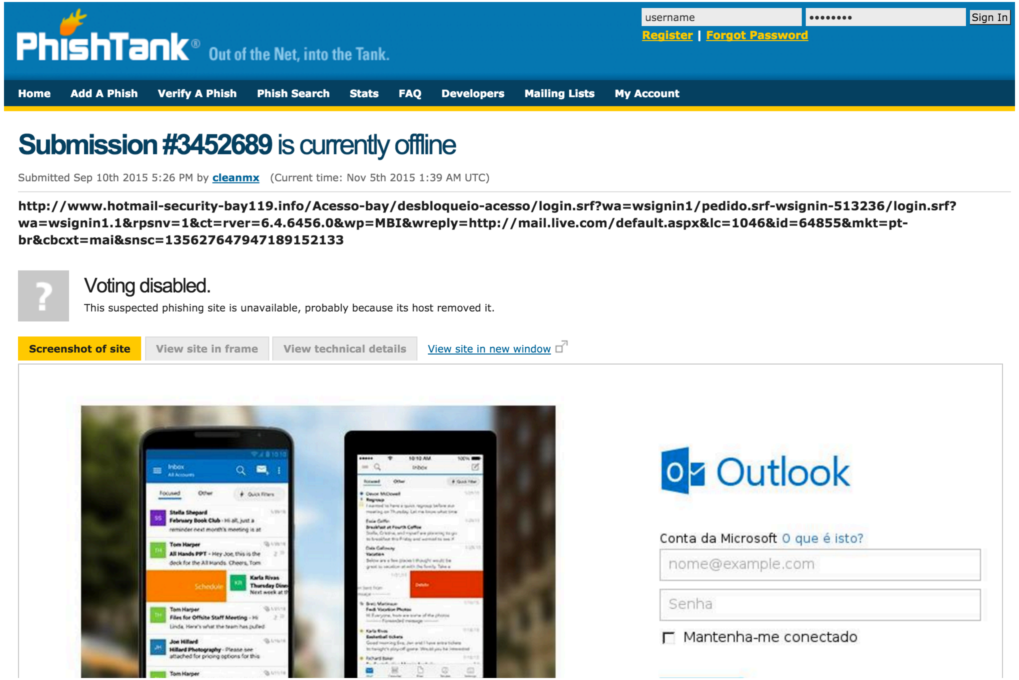
HOSTNAME	FIRST RESOLVED	LAST RESOLVED
wabspedido101.info	Sept. 11, 2015, 1:22 a.m.	Sept. 13, 2015, 3:11 a.m.
hotmail-security-bay119.info	Sept. 2, 2015, 2:50 a.m.	Oct. 4, 2015, 7:02 a.m.
hotmail-security-bay120.info	Sept. 12, 2015, 2:26 a.m.	Sept. 13, 2015, 2:23 a.m.



AMAZON-02 - Amazon.com, Inc.,US (16509)

- Nothing unusual on the domain name data at first glance, and the IP address is located on Amazon
- However, when we review the Passive DNS data on the domain, we find the domains registered are very recent and have slightly suspicious names
- Turns out that hotmail-security-bay119.info had an indirect match on our system just the day before

Ex 1: Detecting By Pivoting On pDNS And WHOIS



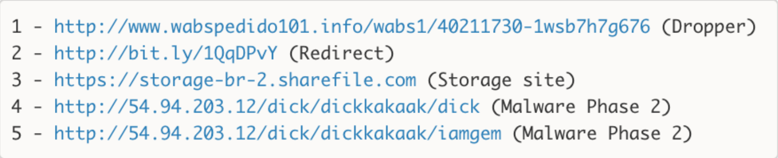
Submission #3452689 is currently offline

Submitted Sep 10th 2015 5:26 PM by cleanmx (Current time: Nov 5th 2015 1:39 AM UTC)

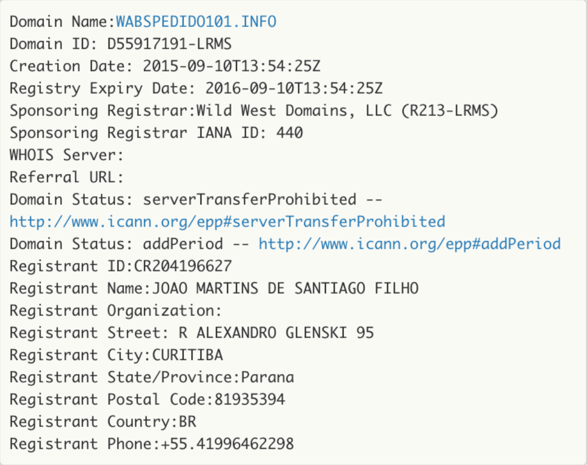
http://www.hotmail-security-bay119.info/Acesso-bay/desbloqueio-acesso/login.srf?wa=wsignin1/pedido.srf-wsignin-513236/login.srf?wa=wsignin1.1&rpsnv=1&ct=rver=6.4.6456.0&wp=MBI&wreply=http://mail.live.com/default.aspx&lc=1046&id=64855&mkt=pt-br&cbcxt=mai&snsc=135627647947189152133

Voting disabled.

This suspected phishing site is unavailable, probably because its host removed it.



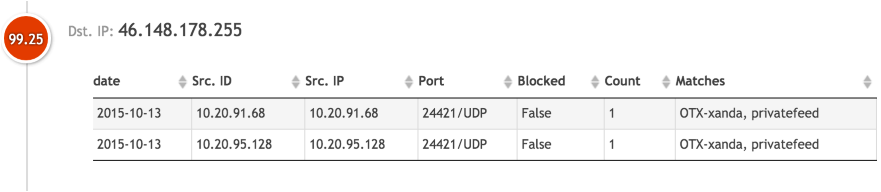
```
1 - http://www.wabspedido101.info/wabs1/40211730-1wsb7h7g676 (Dropper)
2 - http://bit.ly/1QqDPvY (Redirect)
3 - https://storage-br-2.sharefile.com (Storage site)
4 - http://54.94.203.12/dick/dickkakaak/dick (Malware Phase 2)
5 - http://54.94.203.12/dick/dickkakaak/iamgem (Malware Phase 2)
```



```
Domain Name:WABSPEDIDO101.INFO
Domain ID: D55917191-LRMS
Creation Date: 2015-09-10T13:54:25Z
Registry Expiry Date: 2016-09-10T13:54:25Z
Sponsoring Registrar:Wild West Domains, LLC (R213-LRMS)
Sponsoring Registrar IANA ID: 440
WHOIS Server:
Referral URL:
Domain Status: serverTransferProhibited --
http://www.icann.org/epp#serverTransferProhibited
Domain Status: addPeriod -- http://www.icann.org/epp#addPeriod
Registrant ID:CR204196627
Registrant Name:JOAO MARTINS DE SANTIAGO FILHO
Registrant Organization:
Registrant Street: R ALEXANDRO GLENSKI 95
Registrant City:CURITIBA
Registrant State/Province:Parana
Registrant Postal Code:81935394
Registrant Country:BR
Registrant Phone:+55.41996462298
```

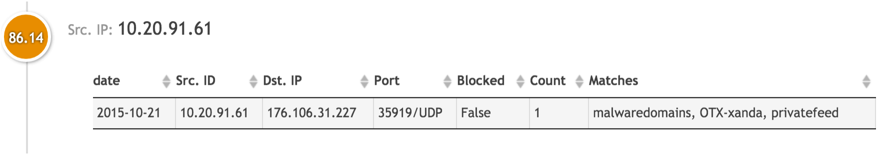
- Analysis of the WHOIS entries showed that they had all been registered under the same information
- The wabspedido101.info only showed in a blacklist (a private one) on 2015-09-16, 4 days after the detection by Magnet

Ex 2: Tracking An Actor's Infrastructure



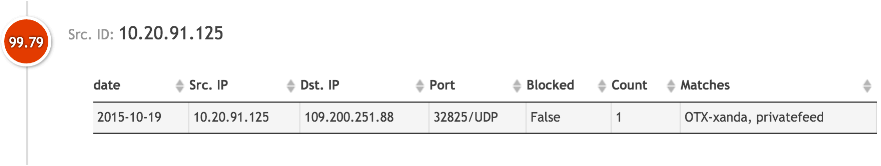
99.25 Dst. IP: 46.148.178.255

date	Src. ID	Src. IP	Port	Blocked	Count	Matches
2015-10-13	10.20.91.68	10.20.91.68	24421/UDP	False	1	OTX-xanda, privatefeed
2015-10-13	10.20.95.128	10.20.95.128	24421/UDP	False	1	OTX-xanda, privatefeed



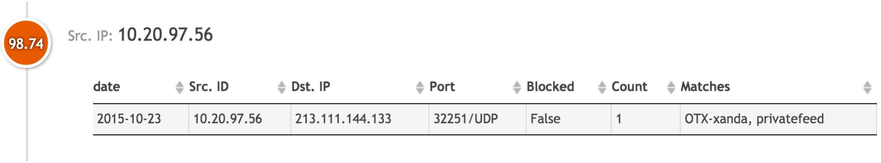
86.14 Src. IP: 10.20.91.61

date	Src. ID	Dst. IP	Port	Blocked	Count	Matches
2015-10-21	10.20.91.61	176.106.31.227	35919/UDP	False	1	malwaredomains, OTX-xanda, privatefeed



99.79 Src. ID: 10.20.91.125

date	Src. IP	Dst. IP	Port	Blocked	Count	Matches
2015-10-19	10.20.91.125	109.200.251.88	32825/UDP	False	1	OTX-xanda, privatefeed

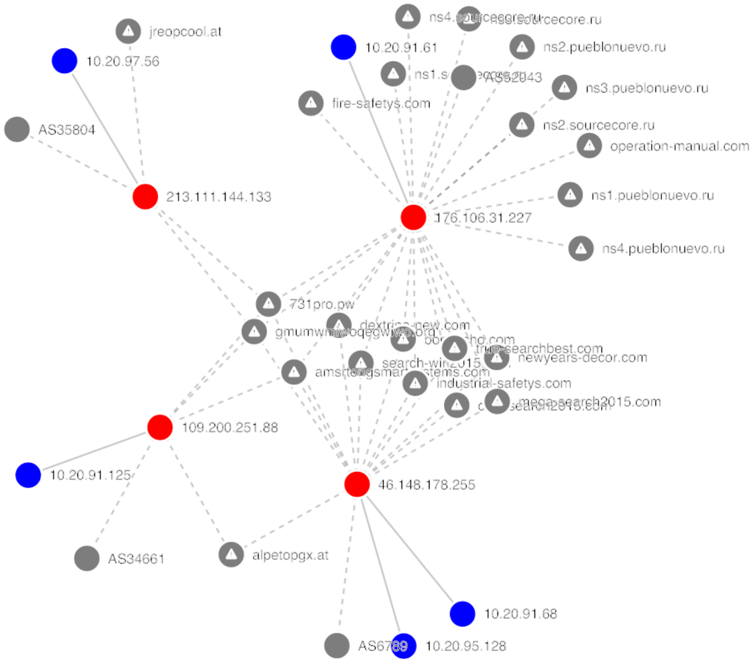


98.74 Src. IP: 10.20.97.56

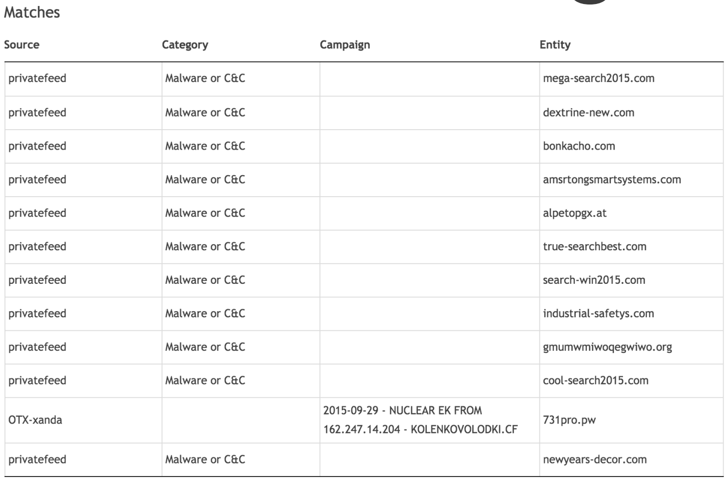
date	Src. ID	Dst. IP	Port	Blocked	Count	Matches
2015-10-23	10.20.97.56	213.111.144.133	32251/UDP	False	1	OTX-xanda, privatefeed

- Suspicious alerts of allowed communications to high UDP ports for destinations in IP addresses in countries prone to bulletproof hosting
- No DNS data from the customer, they had a collection blind-spot on that specific network segment
- Communications to these suspicious IP addresses only happen on that specific day. No repeat IP addresses when changing to a week or month-long view on the portal

Ex 2: Tracking An Actor’s Infrastructure

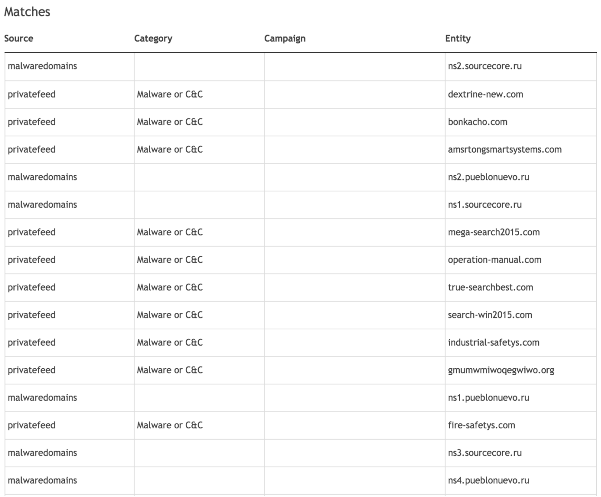


Ex 2: Tracking An Actor's Infrastructure



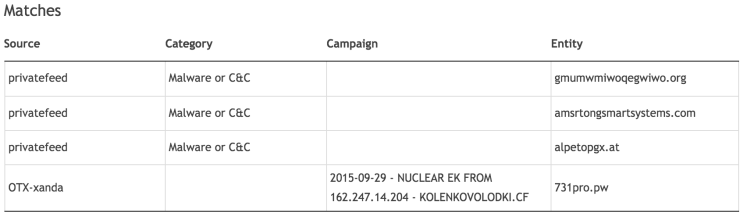
Matches

Source	Category	Campaign	Entity
privatefeed	Malware or C&C		mega-search2015.com
privatefeed	Malware or C&C		dextrine-new.com
privatefeed	Malware or C&C		bonkacho.com
privatefeed	Malware or C&C		amsrtongsmartsystems.com
privatefeed	Malware or C&C		alpetopgx.at
privatefeed	Malware or C&C		true-searchbest.com
privatefeed	Malware or C&C		search-win2015.com
privatefeed	Malware or C&C		industrial-safetys.com
privatefeed	Malware or C&C		gmumwmiwoqegwiwo.org
privatefeed	Malware or C&C		cool-search2015.com
OTX-xanda		2015-09-29 - NUCLEAR EK FROM 162.247.14.204 - KOLENKOVOLODKI.CF	731pro.pw
privatefeed	Malware or C&C		newyears-decor.com



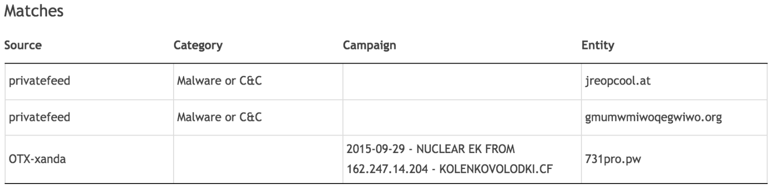
Matches

Source	Category	Campaign	Entity
malwaredomains			ns2.sourcecore.ru
privatefeed	Malware or C&C		dextrine-new.com
privatefeed	Malware or C&C		bonkacho.com
privatefeed	Malware or C&C		amsrtongsmartsystems.com
malwaredomains			ns2.pueblonuevo.ru
malwaredomains			ns1.sourcecore.ru
privatefeed	Malware or C&C		mega-search2015.com
privatefeed	Malware or C&C		operation-manual.com
privatefeed	Malware or C&C		true-searchbest.com
privatefeed	Malware or C&C		search-win2015.com
privatefeed	Malware or C&C		industrial-safetys.com
privatefeed	Malware or C&C		gmumwmiwoqegwiwo.org
malwaredomains			ns1.pueblonuevo.ru
privatefeed	Malware or C&C		fire-safetys.com
malwaredomains			ns3.sourcecore.ru
malwaredomains			ns4.pueblonuevo.ru



Matches

Source	Category	Campaign	Entity
privatefeed	Malware or C&C		gmumwmiwoqegwiwo.org
privatefeed	Malware or C&C		amsrtongsmartsystems.com
privatefeed	Malware or C&C		alpetopgx.at
OTX-xanda		2015-09-29 - NUCLEAR EK FROM 162.247.14.204 - KOLENKOVOLODKI.CF	731pro.pw

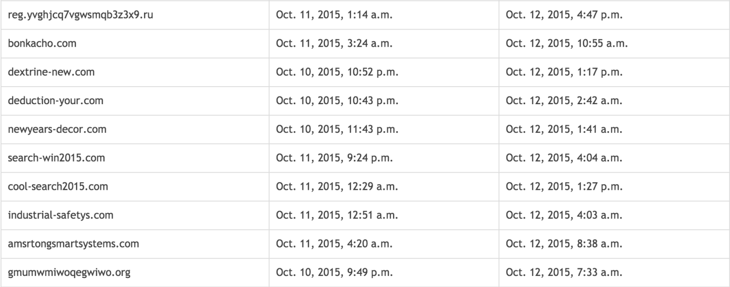


Matches

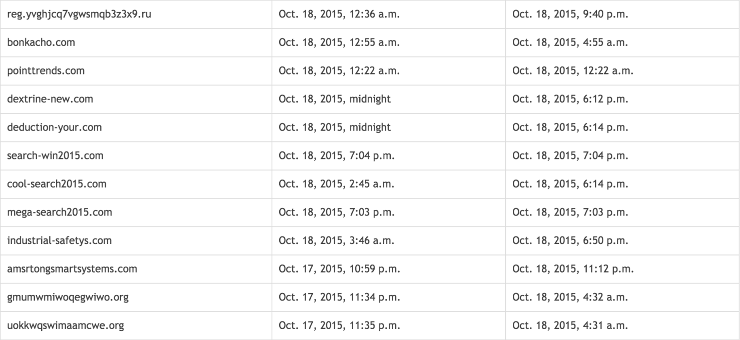
Source	Category	Campaign	Entity
privatefeed	Malware or C&C		jreopcool.at
privatefeed	Malware or C&C		gmumwmiwoqegwiwo.org
OTX-xanda		2015-09-29 - NUCLEAR EK FROM 162.247.14.204 - KOLENKOVOLODKI.CF	731pro.pw

- There were no direct matches on the IP addresses but you can start to see the relationship between the attacks because they have similar indirect matches. It looks like the actor is moving the infrastructure around

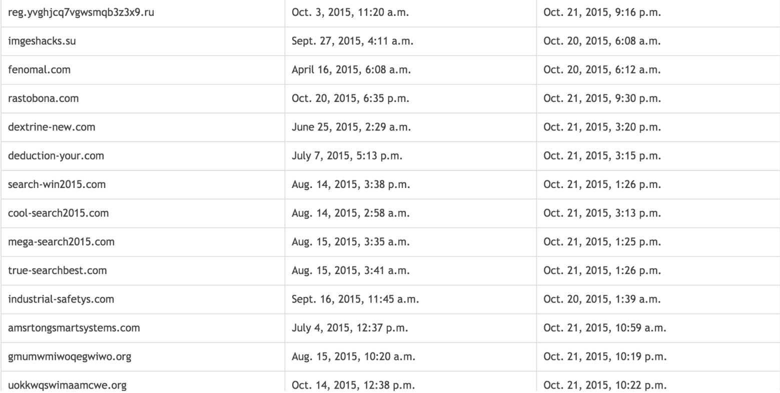
Ex 2: Tracking An Actor’s Infrastructure



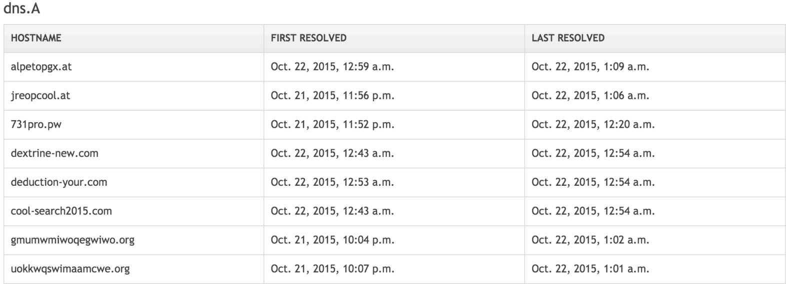
reg.yvghjcq7vgwsmqb3z3x9.ru	Oct. 11, 2015, 1:14 a.m.	Oct. 12, 2015, 4:47 p.m.
bonkacho.com	Oct. 11, 2015, 3:24 a.m.	Oct. 12, 2015, 10:55 a.m.
dextrine-new.com	Oct. 10, 2015, 10:52 p.m.	Oct. 12, 2015, 1:17 p.m.
deduction-your.com	Oct. 10, 2015, 10:43 p.m.	Oct. 12, 2015, 2:42 a.m.
newyears-decor.com	Oct. 10, 2015, 11:43 p.m.	Oct. 12, 2015, 1:41 a.m.
search-win2015.com	Oct. 11, 2015, 9:24 p.m.	Oct. 12, 2015, 4:04 a.m.
cool-search2015.com	Oct. 11, 2015, 12:29 a.m.	Oct. 12, 2015, 1:27 p.m.
industrial-safetys.com	Oct. 11, 2015, 12:51 a.m.	Oct. 12, 2015, 4:03 a.m.
amsrtongsmartsystems.com	Oct. 11, 2015, 4:20 a.m.	Oct. 12, 2015, 8:38 a.m.
gmumwmiwoqegwiwo.org	Oct. 10, 2015, 9:49 p.m.	Oct. 12, 2015, 7:33 a.m.



reg.yvghjcq7vgwsmqb3z3x9.ru	Oct. 18, 2015, 12:36 a.m.	Oct. 18, 2015, 9:40 p.m.
bonkacho.com	Oct. 18, 2015, 12:55 a.m.	Oct. 18, 2015, 4:55 a.m.
pointtrends.com	Oct. 18, 2015, 12:22 a.m.	Oct. 18, 2015, 12:22 a.m.
dextrine-new.com	Oct. 18, 2015, midnight	Oct. 18, 2015, 6:12 p.m.
deduction-your.com	Oct. 18, 2015, midnight	Oct. 18, 2015, 6:14 p.m.
search-win2015.com	Oct. 18, 2015, 7:04 p.m.	Oct. 18, 2015, 7:04 p.m.
cool-search2015.com	Oct. 18, 2015, 2:45 a.m.	Oct. 18, 2015, 6:14 p.m.
mega-search2015.com	Oct. 18, 2015, 7:03 p.m.	Oct. 18, 2015, 7:03 p.m.
industrial-safetys.com	Oct. 18, 2015, 3:46 a.m.	Oct. 18, 2015, 6:50 p.m.
amsrtongsmartsystems.com	Oct. 17, 2015, 10:59 p.m.	Oct. 18, 2015, 11:12 p.m.
gmumwmiwoqegwiwo.org	Oct. 17, 2015, 11:34 p.m.	Oct. 18, 2015, 4:32 a.m.
uokkwqswimaamcwe.org	Oct. 17, 2015, 11:35 p.m.	Oct. 18, 2015, 4:31 a.m.



reg.yvghjcq7vgwsmqb3z3x9.ru	Oct. 3, 2015, 11:20 a.m.	Oct. 21, 2015, 9:16 p.m.
imgeshacks.su	Sept. 27, 2015, 4:11 a.m.	Oct. 20, 2015, 6:08 a.m.
fenomal.com	April 16, 2015, 6:08 a.m.	Oct. 20, 2015, 6:12 a.m.
rastobona.com	Oct. 20, 2015, 6:35 p.m.	Oct. 21, 2015, 9:30 p.m.
dextrine-new.com	June 25, 2015, 2:29 a.m.	Oct. 21, 2015, 3:20 p.m.
deduction-your.com	July 7, 2015, 5:13 p.m.	Oct. 21, 2015, 3:15 p.m.
search-win2015.com	Aug. 14, 2015, 3:38 p.m.	Oct. 21, 2015, 1:26 p.m.
cool-search2015.com	Aug. 14, 2015, 2:58 a.m.	Oct. 21, 2015, 3:13 p.m.
mega-search2015.com	Aug. 15, 2015, 3:35 a.m.	Oct. 21, 2015, 1:25 p.m.
true-searchbest.com	Aug. 15, 2015, 3:41 a.m.	Oct. 21, 2015, 1:26 p.m.
industrial-safetys.com	Sept. 16, 2015, 11:45 a.m.	Oct. 20, 2015, 1:39 a.m.
amsrtongsmartsystems.com	July 4, 2015, 12:37 p.m.	Oct. 21, 2015, 10:59 a.m.
gmumwmiwoqegwiwo.org	Aug. 15, 2015, 10:20 a.m.	Oct. 21, 2015, 10:19 p.m.
uokkwqswimaamcwe.org	Oct. 14, 2015, 12:38 p.m.	Oct. 21, 2015, 10:22 p.m.



dns.A

HOSTNAME	FIRST RESOLVED	LAST RESOLVED
alpetopgx.at	Oct. 22, 2015, 12:59 a.m.	Oct. 22, 2015, 1:09 a.m.
jreopcool.at	Oct. 21, 2015, 11:56 p.m.	Oct. 22, 2015, 1:06 a.m.
731pro.pw	Oct. 21, 2015, 11:52 p.m.	Oct. 22, 2015, 12:20 a.m.
dextrine-new.com	Oct. 22, 2015, 12:43 a.m.	Oct. 22, 2015, 12:54 a.m.
deduction-your.com	Oct. 22, 2015, 12:53 a.m.	Oct. 22, 2015, 12:54 a.m.
cool-search2015.com	Oct. 22, 2015, 12:43 a.m.	Oct. 22, 2015, 12:54 a.m.
gmumwmiwoqegwiwo.org	Oct. 21, 2015, 10:04 p.m.	Oct. 22, 2015, 1:02 a.m.
uokkwqswimaamcwe.org	Oct. 21, 2015, 10:07 p.m.	Oct. 22, 2015, 1:01 a.m.

- Passive DNS data confirms that **Magnet was tracking this actor as it moved their infrastructure**. The IPs never entered threat feeds, and no DNS was available for matching, assuming the domains in question had been listed

4. Integrating Niddel Threat Hunting System And Enterprise Security

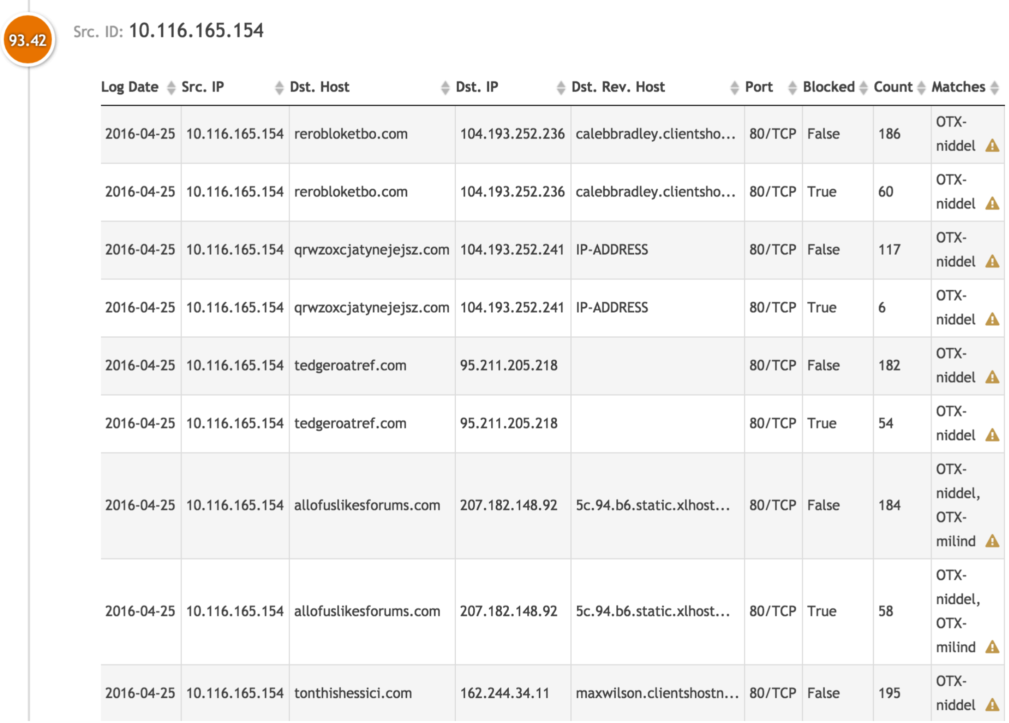
.conf2016

splunk>

Happiness Quote from Greg ☺

”For the first time we are getting value from our firewall logs integrated into our Splunk instance other than on very targeted investigations”

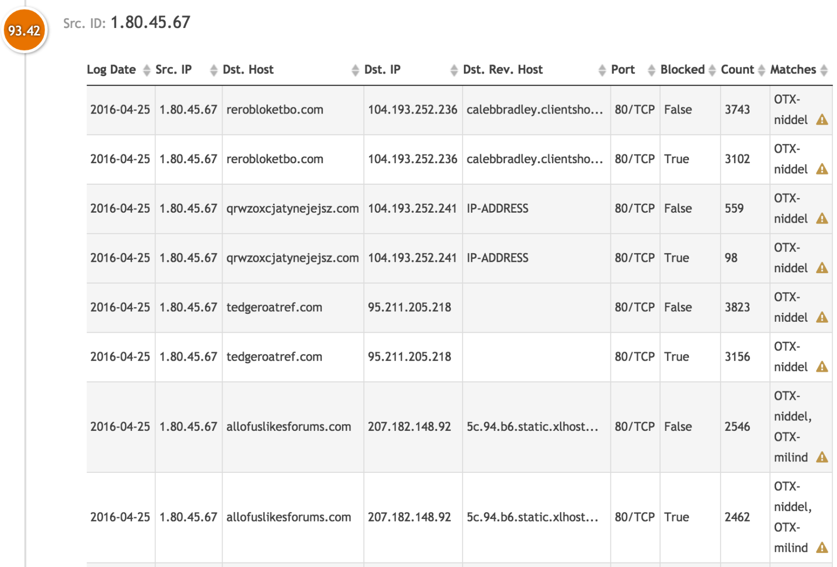
Case Study – Relevant Findings From Niddel App



93.42

Src. ID: 10.116.165.154

Log Date	Src. IP	Dst. Host	Dst. IP	Dst. Rev. Host	Port	Blocked	Count	Matches
2016-04-25	10.116.165.154	rerobloketbo.com	104.193.252.236	calebbradley.clientsho...	80/TCP	False	186	OTX-niddel ⚠
2016-04-25	10.116.165.154	rerobloketbo.com	104.193.252.236	calebbradley.clientsho...	80/TCP	True	60	OTX-niddel ⚠
2016-04-25	10.116.165.154	qrwzoxcjatynejejsz.com	104.193.252.241	IP-ADDRESS	80/TCP	False	117	OTX-niddel ⚠
2016-04-25	10.116.165.154	qrwzoxcjatynejejsz.com	104.193.252.241	IP-ADDRESS	80/TCP	True	6	OTX-niddel ⚠
2016-04-25	10.116.165.154	tedgeroatref.com	95.211.205.218		80/TCP	False	182	OTX-niddel ⚠
2016-04-25	10.116.165.154	tedgeroatref.com	95.211.205.218		80/TCP	True	54	OTX-niddel ⚠
2016-04-25	10.116.165.154	allofuslikesforums.com	207.182.148.92	5c.94.b6.static.xlhost...	80/TCP	False	184	OTX-niddel, OTX-milind ⚠
2016-04-25	10.116.165.154	allofuslikesforums.com	207.182.148.92	5c.94.b6.static.xlhost...	80/TCP	True	58	OTX-niddel, OTX-milind ⚠
2016-04-25	10.116.165.154	tonthishessici.com	162.244.34.11	maxwilson.clientshostn...	80/TCP	False	195	OTX-niddel ⚠



93.42

Src. ID: 1.80.45.67

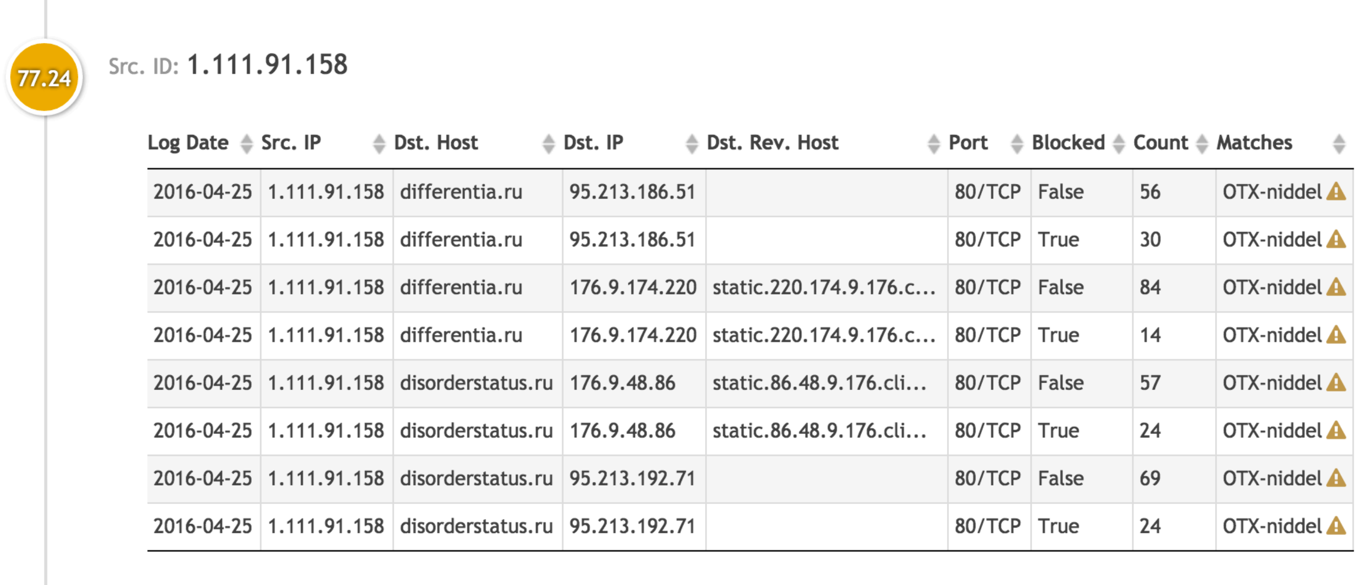
Log Date	Src. IP	Dst. Host	Dst. IP	Dst. Rev. Host	Port	Blocked	Count	Matches
2016-04-25	1.80.45.67	rerobloketbo.com	104.193.252.236	calebbradley.clientsho...	80/TCP	False	3743	OTX-niddel ⚠
2016-04-25	1.80.45.67	rerobloketbo.com	104.193.252.236	calebbradley.clientsho...	80/TCP	True	3102	OTX-niddel ⚠
2016-04-25	1.80.45.67	qrwzoxcjatynejejsz.com	104.193.252.241	IP-ADDRESS	80/TCP	False	559	OTX-niddel ⚠
2016-04-25	1.80.45.67	qrwzoxcjatynejejsz.com	104.193.252.241	IP-ADDRESS	80/TCP	True	98	OTX-niddel ⚠
2016-04-25	1.80.45.67	tedgeroatref.com	95.211.205.218		80/TCP	False	3823	OTX-niddel ⚠
2016-04-25	1.80.45.67	tedgeroatref.com	95.211.205.218		80/TCP	True	3156	OTX-niddel ⚠
2016-04-25	1.80.45.67	allofuslikesforums.com	207.182.148.92	5c.94.b6.static.xlhost...	80/TCP	False	2546	OTX-niddel, OTX-milind ⚠
2016-04-25	1.80.45.67	allofuslikesforums.com	207.182.148.92	5c.94.b6.static.xlhost...	80/TCP	True	2462	OTX-niddel, OTX-milind ⚠

Bedep is a ”click-fraud” botnet.

Successful Bedep infections from Angler EK.

Look at the high number of accesses on the pages!

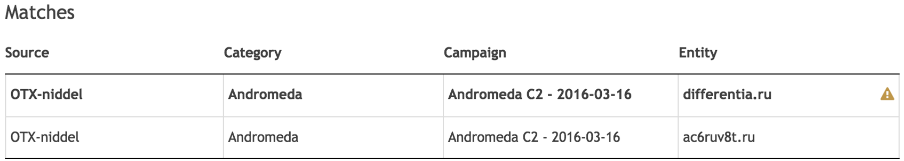
Case Study – Relevant Findings From Niddel App



77.24

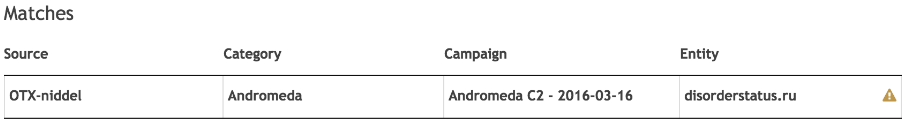
Src. ID: 1.111.91.158

Log Date	Src. IP	Dst. Host	Dst. IP	Dst. Rev. Host	Port	Blocked	Count	Matches
2016-04-25	1.111.91.158	differentia.ru	95.213.186.51		80/TCP	False	56	OTX-niddel ⚠
2016-04-25	1.111.91.158	differentia.ru	95.213.186.51		80/TCP	True	30	OTX-niddel ⚠
2016-04-25	1.111.91.158	differentia.ru	176.9.174.220	static.220.174.9.176.c...	80/TCP	False	84	OTX-niddel ⚠
2016-04-25	1.111.91.158	differentia.ru	176.9.174.220	static.220.174.9.176.c...	80/TCP	True	14	OTX-niddel ⚠
2016-04-25	1.111.91.158	disorderstatus.ru	176.9.48.86	static.86.48.9.176.cli...	80/TCP	False	57	OTX-niddel ⚠
2016-04-25	1.111.91.158	disorderstatus.ru	176.9.48.86	static.86.48.9.176.cli...	80/TCP	True	24	OTX-niddel ⚠
2016-04-25	1.111.91.158	disorderstatus.ru	95.213.192.71		80/TCP	False	69	OTX-niddel ⚠
2016-04-25	1.111.91.158	disorderstatus.ru	95.213.192.71		80/TCP	True	24	OTX-niddel ⚠



Matches

Source	Category	Campaign	Entity
OTX-niddel	**Andromeda**	**Andromeda C2 - 2016-03-16**	**differentia.ru** ⚠
OTX-niddel	Andromeda	Andromeda C2 - 2016-03-16	ac6ruv8t.ru

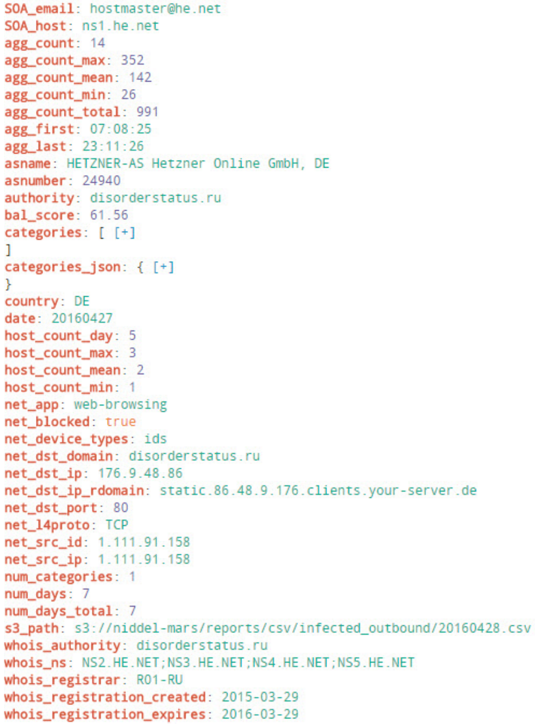


Matches

Source	Category	Campaign	Entity
OTX-niddel	**Andromeda**	**Andromeda C2 - 2016-03-16**	**disorderstatus.ru** ⚠

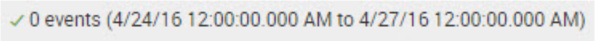
Case Study – Correlation With Other Data

Niddel alert is received



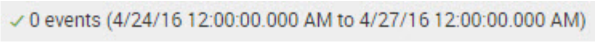
```
SOA_email: hostmaster@he.net
SOA_host: ns1.he.net
agg_count: 14
agg_count_max: 352
agg_count_mean: 142
agg_count_min: 26
agg_count_total: 991
agg_first: 07:08:25
agg_last: 23:11:26
asname: HETZNER-AS Hetzner Online GmbH, DE
asnumber: 24940
authority: disorderstatus.ru
bal_score: 61.56
categories: [ [+]
]
categories_json: { [+]
}
country: DE
date: 20160427
host_count_day: 5
host_count_max: 3
host_count_mean: 2
host_count_min: 1
net_app: web-browsing
net_blocked: true
net_device_types: ids
net_dst_domain: disorderstatus.ru
net_dst_ip: 176.9.48.86
net_dst_ip_rdomain: static.86.48.9.176.clients.your-server.de
net_dst_port: 80
net_l4proto: TCP
net_src_id: 1.111.91.158
net_src_ip: 1.111.91.158
num_categories: 1
num_days: 7
num_days_total: 7
s3_path: s3://niddel-mars/reports/csv/infected_outbound/20160428.csv
whois_authority: disorderstatus.ru
whois_ns: NS2.HE.NET;NS3.HE.NET;NS4.HE.NET;NS5.HE.NET
whois_registrar: R01-RU
whois_registration_created: 2015-03-29
whois_registration_expires: 2016-03-29
```

Correlated with Endpoint AV data →



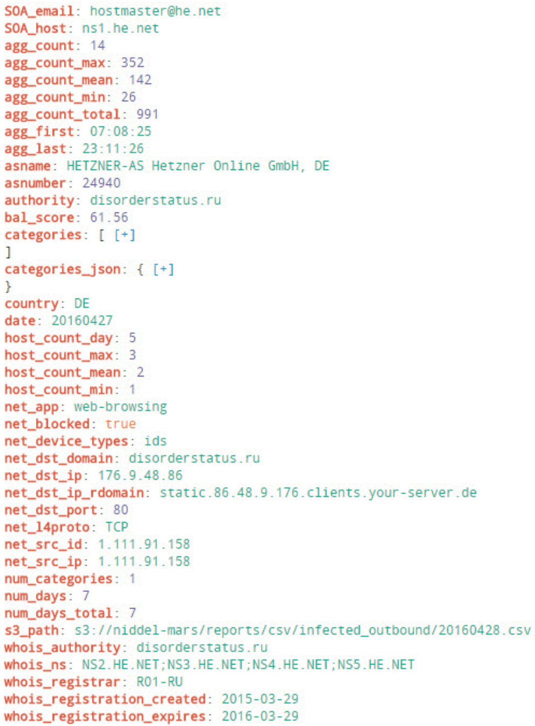
✓ 0 events (4/24/16 12:00:00.000 AM to 4/27/16 12:00:00.000 AM)

Correlated with IDS data →



✓ 0 events (4/24/16 12:00:00.000 AM to 4/27/16 12:00:00.000 AM)

Case Study – ES Dashboard Prioritization



```
SOA_email: hostmaster@he.net
SOA_host: ns1.he.net
agg_count: 14
agg_count_max: 352
agg_count_mean: 142
agg_count_min: 26
agg_count_total: 991
agg_first: 07:08:25
agg_last: 23:11:26
asname: HETZNER-AS Hetzner Online GmbH, DE
asnumber: 24940
authority: disorderstatus.ru
bal_score: 61.56
categories: [ [+]
]
categories_json: { [+]
}
country: DE
date: 20160427
host_count_day: 5
host_count_max: 3
host_count_mean: 2
host_count_min: 1
net_app: web-browsing
net_blocked: true
net_device_types: ids
net_dst_domain: disorderstatus.ru
net_dst_ip: 176.9.48.86
net_dst_ip_rdomain: static.86.48.9.176.clients.your-server.de
net_dst_port: 80
net_l4proto: TCP
net_src_id: 1.111.91.158
net_src_ip: 1.111.91.158
num_categories: 1
num_days: 7
num_days_total: 7
s3_path: s3://niddel-mars/reports/csv/infected_outbound/20160428.csv
whois_authority: disorderstatus.ru
whois_ns: NS2.HE.NET;NS3.HE.NET;NS4.HE.NET;NS5.HE.NET
whois_registrar: R01-RU
whois_registration_created: 2015-03-29
whois_registration_expires: 2016-03-29
```

New priority rules can be based on many factors:

- Session count
- Score
- Firewall action (Blocked or Not Blocked)
- WHOIS Age
- Correlation with associated sources from the endpoint and network

5. Conclusion/Takeaways

Key Takeaways

- Threat Intelligence can be a very powerful detection tool, but the way it is presented today is incomplete for effective usage

- Threat Hunting is being implemented as a analyst-intensive process to make that data work on detection processes

- The real promise of having IOC data as a reliable detection technique comes from pivoting and learning from it. Making that scalable is the real challenge

Want To Learn More On Hunting/TI?

- **Niddel** – http://www.niddel.com/
- **MLSec Project** – http://www.mlsecproject.org/
- **Threat Hunting Resources** - http://www.threathunting.net/
- **Splunk ES Threat Intelligence Dashboards** - http://docs.splunk.com/Documentation/ES/4.2.0/User/ThreatIntelligence
- **Splunk ES WHOIS and Threat Intelligence Integration** - http://docs.splunk.com/Documentation/ES/4.2.0/User/ThreatListActivitydashboard

Q&A/Feedback

THANK YOU

.conf2016

splunk>